REMARKS

The Office Action received April 16, 2009, has been received and carefully considered. Reconsideration of the current rejections in the present application is respectfully requested based on the following remarks.[1]

I. REQUEST FOR RECONSIDERATION OF THE RESTRICTION REQUIREMENT CONSISTENT WITH REQUIREMENTS SET FORTH IN 37 C.F.R. §§ 1.143

On page 2 of the Office Action, the Examiner asserts that the present application contains claims directed to two patentably distinct species of the claimed invention: one species directed to "Originally filed claim 5," and another species directed to claims 1 and 3-11. The second species includes current claim 5. The Applicant hereby respectfully traverses this election/restriction requirement and hereby requests that the Examiner reconsider and withdraw this election/restriction requirement. Applicant is unable to

[1] As Applicant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicant's silence as to assertions made by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., assertions regarding dependent claims, whether a reference constitutes prior art, whether references are legally combinable for obviousness purposes) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute such in the future.

provisionally elect a species as the Examiner has made a constructive election and therefore not afforded Applicant that option.

The Examiner sets forth a restriction requirement that is not only improper, but incomprehensible. Additionally, the Examiner unilaterally withdraws claims from consideration and attempts to justify this maneuver with cites to 37 CFR 1.142(b) and MPEP § 821.03,[2]

A. The Improper and Incomprehensible Restriction Requirement

The restriction requirement is grounded in neither law nor USPTO policy. Under 35 U.S.C. § 121, restriction is appropriate if two or more independent and distinct inventions are claimed in one application. As set forth in MPEP § 802.01, inventions are independent if there is no disclosed relationship between the two or more subjects disclosed, and inventions are distinct if two or more subjects as disclosed are capable of separate manufacture, use, or sale as claimed.

The Examiner restricts originally filed claim 5 from claim 1. Claim 5 is a dependent claim. It currently depends from claim 1 directly. As originally filed, it was indirectly

[2] The cited passages do not support the Examiner's position. They speak to restriction practice of newly added claims. The present claims are not newly added. Indeed, they were not even presently amended.

dependent on claim 1. Thus, by definition, it is not independent. For at least these reasons, the restriction requirement is improper and Applicant respectfully requests the withdrawal of the same.

Further, the Examiner has not provided any reasons why examination of the claims "would be a serious burden on the Examiner." MPEP 808.01(A). The fact that all of the claims have been examined on the merits through several rounds of prosecution and were presented to the Examiner in the previous response without amendment significantly weakens any potential argument that examination of the claims presented a serious burden that required a restriction requirement.

The restriction requirement is additionally improper because it lists two species and includes a generic claim in one of the species. A claim cannot be a genus and a species at the same time.

The restriction requirement is also incomprehensible. Claim 5 is included in both species. Is the Examiner alleging that currently recited claim 5 is independent and distinct from the original claim 5? What, then, is Species 1? What is being restricted? And on what basis? There cannot be a species restriction requirement if there is only one species. And yet the Examiner is requiring a restriction among a group of claims

that the Examiner acknowledges belong to the same species.

B. The Improper Withdrawal By Way of "Constructive Election" of Claims 1 and 3-11

The restriction requirement – and, indeed, the Office Action in general -- is improper because the Examiner withdrew from consideration claims 1 and 3-11 without consent from the Applicant. The Examiner states that "Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits." The Examiner cites to 37 CFR 1.142(b) and MPEP § 821.03 as allegedly justifying this requirement. Indeed, the above quote is the second paragraph of form paragraph from Section 821.03. The Examiner omitted the first paragraph, which states "Newly submitted claim … directed to an invention that is independent or distinct from the invention originally claimed for the following reasons …"

MPEP § 821.03 clearly only applies to "claims added by amendment following action by the Examiner."[3] This is even stated in the heading of Section 821.03. No new claims have been added. Thus, this situation does not exist here. Applicants

[3] Indeed Section 821.03 is entitled "Claims for Different Invention Added After an Offic Action."

respectfully submit that these claims have been improperly withdrawn from consideration. Applicant respectfully requests correction of this improper maneuver so that these claims may be further considered on the merits and the application may be forwarded toward allowance.

II. THE NON-STATUTORY REJECTION OF CLAIMS 12-19

On Page 3 of the Office Action, claims 12-19 were rejected under 35 U.S.C. 101 because the claimed invention is allegedly directed to non-statutory subject matter. This rejection is hereby respectfully traversed.

"A claimed process is patent-eligible under § 101 if: (1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing." In re Bilski, 545 F.3d 943, 954 (Fed. Cir. 2008). That is, "a claimed process involving a fundamental principle that uses a particular machine or apparatus would not pre-empt uses of the principle that do not also use the specified machine or apparatus in the manner claimed." Id. Also, "a claimed process that transforms a particular article to a specified different state or thing by applying a fundamental principle would not pre-empt the use of the principle to transform any other article, to transform the same article but in a manner not

covered by the claim, or to do anything other than transform the specified article." Id. Thus, "a claim that is tied to a particular machine or brings about a particular transformation of a particular article does not pre-empt all uses of a fundamental principle in any field but rather is limited to a particular use, a specific application." Id. at 957. However, even if a claim recites a specific machine or a particular transformation of a specific article, the recited machine or transformation must not constitute mere "insignificant postsolution activity." Id.

Claim 12 has been amended to recite a "computer implemented" method, thus explicitly tying the method to a machine or apparatus. Further, claim 12 is statutory in that various recitations of the claim, e.g. "encrypting the masked XOR-sum using a block cipher and a first key," satisfy both criteria in that a particular article into a different state or thing (e.g., plaintext is transformed into ciphertext) and is tied to an apparatus (e.g., a block cipher is performed on a hardware logic circuit or on coded computer readable media). Thus, not one, but both requirements under the current case law are met. Accordingly, claim 12 is directed to statutory subject matter and withdrawal of the rejection is respectfully requested.

Claims 13-19 depend from claim 12 and are statutory at least as a result of this dependency.

In view of the foregoing, it is respectfully requested that the aforementioned rejection of claims 12-19 be withdrawn.

III. THE OBVIOUSNESS REJECTION OF CLAIMS 12-20

On pages 3-7 of the Office Action, claims 12-20 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Rogaway ("OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption") in view of Schneier ("Applied Cryptography, Second Edition"). This rejection is hereby respectfully traversed.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074 (Fed. Cir. 1988). There are four separate factual inquiries to consider in making an obviousness determination: (1) the scope and content of the prior art; (2) the level of ordinary skill in the field of the invention; (3) the differences between the claimed invention and the prior art; and (4) the existence of any objective evidence, or "secondary considerations," of non-obviousness. Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966); see also KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007). An "expansive and flexible

approach" should be applied when determining obviousness based on a combination of prior art references. KSR, 127 S. Ct. at 1739. However, a claimed invention combining multiple known elements is not rendered obvious simply because each element was known independently in the prior art. Id. at 1741. Rather, there must still be some "reason that would have prompted" a person of ordinary skill in the art to combine the elements in the specific way that he or she did. Id.; In re Icon Health & Fitness, Inc., 496 F.3d 1374, 1380 (Fed. Cir. 2007). Also, modification of a prior art reference may be obvious only if there exists a reason that would have prompted a person of ordinary skill to make the change. KSR, 127 S. Ct. at 1740-41.

The Examiner asserts that the claimed invention would have been obvious in view of the combination of Rogaway and Schneier. Applicant respectfully disagrees.

Rogaway does not disclose any function that could be analogized to the presently claimed application of an XOR function to all message blocks of a message. Further, Rogaway fails to disclose, or even suggest, any value that could be analogized to the presently claimed XOR-sum.

The Examiner (see Office Action, pg. 3) also alleges that the Rogaway disclosure of concatenating message blocks meets the recited claim 12 element of applying an XOR function to all

message blocks of a message to compute an XOR-sum. The Examiner states "concatenation effectively creates the XOR-sum." Applicant disagrees that the concatenation described in Rogaway meets this claim element. A concatenation operation is very different from an XOR operation in both form and result. Applicant respectfully requests withdrawal of the rejection.

Furthermore, Rogaway also discloses applying a string L and an offset Z[m] to one string of a message M before a block cipher E_K, as well as applying the same message string M[m] after the block cipher E_K (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Additionally, Rogaway also discloses applying an offset Z[m] to a checksum before a block cipher E_K, and then limiting the block cipher result to a tag length τ (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Regarding combining Schneier with Rogaway, such a combination would result in an inoperable methodology since replacing the result of encrypting of Rogaway with an additional XOR function as mentioned by Schneier would not result in a limited tag length τ, which is required by Rogaway.

In view of the foregoing, it is respectfully submitted that claim 12 is allowable over the combination of Rogaway and Schneier.

Regarding claims 13-20, these claims are dependent upon independent claim 12. Thus, since independent claim 12 should be allowable as discussed above, claims 13-20 should also be allowable at least by virtue of their dependency on independent claim 12. Moreover, these claims recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, it is respectfully requested that the aforementioned obviousness rejection of claims 12-20 be withdrawn. III.

CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: _____
Thomas E. Anderson
Registration No. 37,063

TEA/ple

1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: July 16, 2009